MTR130411

MITRE TECHNICAL REPORT

Formal Modeling of Diffie-Hellman Derivability for Exploratory Automated Analysis

June 2013

Moses D. Liskov
F. Javier Thayer

Sponsor:	**NSA/R2D**	**Contract No.:**	**W15P7T-12-C-F600**
Dept. No.:	**G026**	**Project No.:**	**0713N6BZ**

MITRE
Center for Integrated Intelligence Systems
Bedford, Massachusetts

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2013		**00-00-2013 to 00-00-2013**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Formal Modeling of Diffie-Hellman Derivability for Exploratory Automated Analysis	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **MITRE Corporation,Center for Integrated Intelligence Systems,202 Burlington Road,Bedford,MA,01730**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**20**	

Approved by:

Paul Rowe, 0713N6BZ Project Leader

1. Introduction

In their groundbreaking paper, Diffie and Hellman[3] proposed the first public-key operation, now known as the Diffie-Hellman key agreement protocol. Over three decades later, this protocol remains crucially important, a component of a great many cryptographic protocols.

In this paper we compare several models that capture the Diffie-Hellman protocol, with the aim of identifying a model that is both well-suited for automated protocol analysis and that has a strong, well-justified link to the model typically adopted in the computational complexity community. The core goal of any such model is to express the concept of *derivability*: values that can be produced by the model attacker. We start with the computational complexity view of a non-uniform adversary, in which derivability is defined by what can be computed with non-negligible probability by a polynomially bounded non-uniform family of circuits.

We make two changes to this model: we replace computability with a Dolev-Yao style adversary, and we use non-standard analysis techniques to reduce the parametrized asymptotic setting to a simpler, singular one. The use of non-standard analysis helps justify our use of a hyperfinite field of exponents.

Unfortunately, the formal model that results is not usable for automated analysis. First, as shown by Dougherty and Guttman[4], it is not a well-behaved message algebra. Worse, any reasonable attempt at emulating this formal model with an algebra would be problematic because the exponents would form a ring structure, and unification, a key technique in automated exploratory protocol analysis, is not known to be decidable for rings. Thus, we restrict our formal model to a weaker one which does not capture exponent addition or group multiplication.

This would seem to be a problematic model: it seems to deny the adversary some abilities that computability clearly includes, such as the ability to add exponents and multiply bases. Thus, it is open for criticism on the basis that it captures a smaller range of adversarial behavior than the previous model. We show that while this smaller model is less expressive and thus can be used to describe a smaller range of derivability statements, all derivability statements describable in the smaller model that are true in the larger model are true in the smaller model. In other words, the criticism is not well-justified: the only loss in using this smaller model is in restricting the type of statements it can describe. And since this smaller model is still capable of expressing the Diffie-Hellman protocol itself, it is of interest.

1.1. Our results.

Figure 1 gives a diagram describing the various models we discuss in this paper. A is the purely computational model, discussed in Section 2. In Section 3, we give an introduction to non-standard analysis. In Section 4, we discuss the model B obtained by applying a non-standard analysis "limit" to the computational model. In Section 5 we discuss the process of formalizing our models. C is obtained via a minimal and natural formalization of the computational model, while D is obtained from C by applying a non-standard limit to C. However, D can also be constructed in a simpler way by a more radical formalization of B. In Section 5 we prove one of our two main results: that these two models are equivalent, so the simpler version of D may be regarded as the result of a minimal formalization of the computational model. In Sections 6 and 7 we prove the main technical lemmas supporting this result. Finally, in Section 8 we discuss the

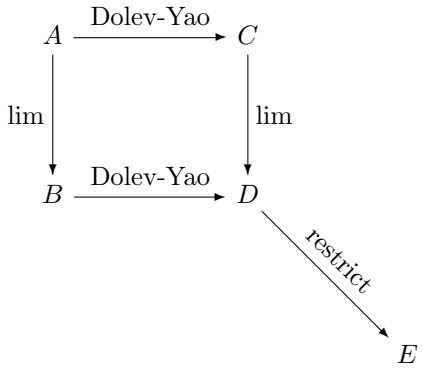

FIGURE 1. Relationships among various Diffie-Hellman models we discuss.

restriction of the resulting model to our Diffie-Hellman algebra and prove our other main result: a conservative extension relationship between the restricted and full Diffie-Hellman models.

2. Diffie-Hellman

The Diffie-Hellman protocol is described in a finite group G of prime order $\mathrm{Ord}(G) = p$, along with a generator g. It is believed that in such groups the "discrete logarithm problem" of finding a random x given (G, g, g^x) is hard. It is further believed that if x and y are random, it is hard to find g^{xy} given (G, g, g^x, g^y); this is called the computational Diffie-Hellman problem.

The hardness of these computational problems is the basis of Diffie-Hellman key exchange and many other cryptographic techniques. There are certain aspects of the standard computational model in which statements of the tractibility or intractibility of such problems are stated that need to be reviewed here. In particular, it is important to state the computational hardness of such problems in a way that seems realistic.

First of all, such statements are asymptotic ones. These problems may be solved via brute force if the prime order p is small enough. Thus, any asymptotic definition will necessarily include an infinite family of p, G, and g. However, one attractive feature of discrete logarithm-based crytography is that no "trap-door" is thought to exist making the discrete logarithm problem or the computational Diffie-Hellman problem easy under a given set of parameters. Thus, the same parameters can be used by everyone.

Second, hardness is meant to be as close as possible to impossibility, but we must recognize that randomized algorithms will always be able to have a tiny chance of success, for instance, by guessing the right answer at random. Thus, the standard computational model concerns problems that can be solved with non-negligible probability.

2.1. Preliminaries and notation.

The expression $\Pr[v_1 \leftarrow A_1; \ldots; v_n \leftarrow A_n : P(v_1, \ldots, v_n)]$ refers to the probability that $P(v_1, \ldots, v_n)$ holds given assignment of each of v_1 through v_n based on probability distributions $A_1, \ldots, A_n$. When a finite set is given in place of a probability distribution, the uniform distribution on

that set is implied. When an algorithm is in place of a probability distribution, it is implied that a run of that algorithm is performed, with uniform randomness if the algorithm is randomized.

A *rational expression with integer coefficients* is an element of the field of quotients of the polynomial ring $\mathbb{Z}[x_1, \ldots, x_n]$. We denote it by $\mathbb{Z}(x_1, \ldots, x_n)$. A *monomial* is an expression of the form $M(\bar{x}) = \bar{x}^{\bar{\alpha}} = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ where $n \in \mathbb{N}$ and $\alpha_i \in \mathbb{Z}$. We associate to the monomial M the function (which by abuse of language we also denote by M) $\bar{a} \mapsto a_1^{\alpha_1} \cdots a_n^{\alpha_n}$ defined whenever all $a_i \neq 0$.

We use a bar to indicate a sequence of values. Thus, we may describe a particular rational expression as $R(\bar{x})$, which leaves ambiguous the value of n such that $R \in \mathbb{Z}(x_1, \ldots, x_n)$. If $\bar{R}$ is a sequence of rational expressions $\bar{R} = R_1, \ldots, R_n$, we can use $\bar{R}(\bar{x})$ to refer to $(R_1(\bar{x}), \ldots, R_n(\bar{x}))$ and $g^{\bar{R}(\bar{x})}$ to refer to $(g^{R_1(\bar{x})}, \ldots, g^{R_n(\bar{x})})$.

Let $(\bar{R}_0, \bar{R}_1)$ be a pair of sequences of rational expressions each on the same number of inputs. Whenever we have a space of base values $\mathcal{B}$ along with an exponentiation operation $\mathcal{B} \times \mathbb{Z} \to \mathcal{B}$, and a distinguished base g, we can define $\bar{R} : \mathbb{Z}^k \to \mathcal{B}^m \times \mathbb{Z}^n$ by $\bar{R}(\bar{x}) = (g^{\bar{R}_0(\bar{x})}, \bar{R}_1(\bar{x}))$. We call such a pair $(\bar{R}_0, \bar{R}_1)$ an *information function*.

Systems of exponent environments. Let G be a cyclic group of prime order p. Since G is of prime order, every $g \in G$ such that $g \neq 1_G$ is a generator for G. In particular, exponentiation is a mapping $G \times \mathbb{Z} \to G$. However, since g^k depends only on the equivalence class of k modulo p, we can view exponentiation as a mapping $G \times \mathbb{Z}/(p) \to G$. We thus view the set of exponents as a field. Suppose G_k is a sequence of such cyclic groups where each G_k is of prime order p_k, such that $p_k \to \infty$. Assume that g_k is a sequence of generators for each G_k.

Definition 2.1. A sequence $\mathcal{S} = \{(G_k, g_k, p_k) : k \in \mathbb{N}\}$ is an *admissible system of exponentiation environments* if G_k is a cyclic group of prime order p_k, where g_k is a generator, and there are constants $0 < c \leq C < \infty$ such that $c\ 2^k \leq p_k \leq C\ 2^k$.

Remark 2.2. It is clear that the exponential growth assumption on p_k is equivalent to the inequality

$$a \log p_k - b \leq k \leq A \log p_k - B \tag{1}$$

for some positive constants a, b, A, B.

In this paper we are concerned with whether certain values can be derived from certain other values. We restrict to a class of such problems in which the information provided and the values to be derived are both based on rational expressions in the exponent.

Definition 2.3. Given an admissible system $\mathcal{S}$ of exponentiation environments, a *derivation problem* for $\mathcal{S}$ is a pair of information functions $((\bar{\alpha}_0, \bar{\alpha}_1), (\bar{\beta}_0, \bar{\beta}_1))$, representing the problem of deriving $\bar{R}(\beta)$ from $\bar{R}(\alpha)$.

Example 2.4. The discrete logarithm problem has $\alpha_0(x) = x$, $\beta_1(x) = x$, and α_1 and β_0 empty sequences. Thus, $\bar{\alpha}(x) = g^x$ and $\bar{\beta}(x) = x$.

Example 2.5. The computational Diffie-Hellman problem has $\alpha_0(x_1, x_2) = (x_1, x_2)$ and $\beta_0(x_1, x_2) = x_1 x_2$, and α_1 and β_1 both empty sequences. Thus, $\bar{\alpha}(x_1, x_2) = (g^{x_1}, g^{x_2})$ and $\bar{\beta}(x_1, x_2) = g^{x_1 x_2}$.

2.2. **Computational model of derivability.** In order to define the computational view of when a derivation problem is solvable, we must introduce two concepts: the notion of a polynomially bounded non-uniform randomized circuit family, and the notion of a negligible function. Roughly, a circuit is a composition of a finite number of NAND gates. The size of a circuit is the number of NAND gates. Each circuit is the implementation of a unique function $\{0,1\}^l \to \{0,1\}^{l'}$. $\mathcal{C}$ denotes the class of circuits.

A set $\{A_k | k \in \mathbb{N}\}$ of circuits is a non-uniform circuit family. Let $\mathcal{NC}$ be the set of non-uniform circuit families.

A non-uniform circuit family $\{A_k\}$ is *polynomially bounded* if there exists a polynomial $\rho(k)$ such that for all k, $|A_k| \leq \rho(k)$. Let $\mathcal{PNC}$ be the set of polynomially bounded non-uniform circuit families.

We may think of circuits as randomized in the sense that some inputs may be preserved for random bits. Computation by randomized polynomially-bounded non-uniform circuit families is the most general standard notion for security of discrete logarithm-based cryptographic schemes.[2] The non-uniform stipulation is important to model security where parameters are reused as they often are for Diffie-Hellman. This scenario is a bit more complex than the more typical case of computation by a probabilistic polynomial-time Turing machine, because that amounts to a *uniform* family of circuits rather than a non-uniform one.

Negligible functions. A function $f : \mathbb{N} \longrightarrow \mathbb{R}$ is *negligible* if and only if for every positive n there is a positive constant C such that $|f(k)| \leq Ck^{-n}$. This is equivalent to the form preferred in the cryptography literature:

$$\forall n \in \mathbb{N}\ \exists k_0\ \forall k \geq k_0\ |f(k)| \leq k^{-n} \tag{2}$$

Condition (2) clearly implies negligibility. Conversely, if f is negligible, for positive n there is a C such that $|f(k)| \leq Ck^{-(n+1)}$ for all k. Let k_0 be such that $Ck_0^{-1} \leq 1$. Then $|f(k)| \leq k^{-n}$. Contrapositively, a function is f *non-negligible* if and only if there are n and infinitely many k such that $|f(k)| \geq k^{-n}$.

It is essential to consider the non-uniform case to capture the assumption that there do not exist trapdoors for the common parameters.

Definition 2.6. A derivation problem $(\bar{\alpha}, \bar{\beta})$ is *solvable* if:

$$\exists \{A_k\} \in \mathcal{PNC} : \Pr[\bar{x} \leftarrow (\mathbb{Z}/(p_k))^n; v \leftarrow A_k(\bar{\alpha}(\bar{x})) : v = \beta(\bar{x})] \text{ is non-negligible.}$$

This notion of solvable gives us a natural corresponding notion of "hard": namely, a derivability problem is hard if it is not solvable.

3. Review of Non-standard Analysis

Our reference for non-standard analysis is [1]. The main constituents of non-standard analysis are a pair of universes $\mho$ and ${}^\circ\mho$ and an operator ${}^\bullet : \mho \longrightarrow {}^\circ\mho$ called an *enlargement operator*. The *transfer principle* is the fact that the operator ${}^\bullet$ preserves the validity of first order formulas. Mathematical terms such as function, cardinality, finiteness, field can be carried over to ${}^\circ\mho$ and the enlargement operator preserves their basic properties. We will refer to $\mho$ as the *standard universe* and ${}^\circ\mho$ as the *non-standard universe*. The transfer principle is stated as follows:

$\mathcal{U}$	${}^\circ\mathcal{U}$	$\mathcal{U}$	${}^\circ\mathcal{U}$
$\in$	$\in$	$\mathbb{N}$	${}^\bullet\mathbb{N}$
$\subseteq$	$\subseteq$	$\mathbb{R}$	${}^\bullet\mathbb{R}$
$\bigcup$	$\bigcup$	$\sum$	${}^\bullet\sum$
$(\cdot,\cdot)$	$(\cdot,\cdot)$	$\prod$	${}^\bullet\prod$
$\mathcal{P}$	${}^\bullet\mathcal{P}$	function	function
card	${}^\bullet$card	finite	${}^\bullet$finite

TABLE 1. Translation Table for Relations, Operators and Predicates

3.1 (Transfer). If $\Phi(x_1,\ldots,x_n)$ is a formula with bounded quantification whose free variables are among $x_1,\ldots,x_n$, then for $a_1,\ldots,a_n \in \mathcal{U}$, $\Phi(a_1,\ldots,a_n)$ is valid in $\mathcal{U}$ if and only if $\Phi({}^\bullet a_1,\ldots,{}^\bullet a_n)$ is valid in ${}^\circ\mathcal{U}$.

By formula we mean first order formula with the predicate symbols "$\in$" and "$=$" and some constants such as 1 and $\mathbb{N}$. The restriction to bounded formulas is not strictly necessary, but it allows us to assume that the model ${}^\circ\mathcal{U}$ interprets the membership operator as $\in$. The reference [1] follows this approach while [6] allows for unrestricted quantifiers.

We could build a correspondence table between symbols in the standard universe and symbols in the non-standard one. To each construct (predicate, operator, relation) C in the standard universe corresponds a construct ${}^\bullet C$ in the non-standard universe. The table would look something like the table in Figure 1. The notations that are used in practice differ from those in this list. For example, for the predicates ${}^\bullet$finite, ${}^\bullet$integer, ${}^\bullet$real we use *hyperfinite, hyperinteger, hyperreal* respectively, A partial mapping $\varphi : {}^\circ\mathcal{U} \longrightarrow {}^\circ\mathcal{U}$ is *internal* if there is an $f \in {}^\circ\mathcal{U}$ satisfying the function predicate such that $\varphi(a)$ is defined if and only if $a \in {}^\bullet\mathrm{dom} f$ and for such values of a, $\varphi(a) = f(a)$. Otherwise, the mapping is said to be *external*. A set is internal (respectively external) if and only if its indicator function is internal (respectively external).

Elements r of the field $\mathbb{C}$ of complex numbers are identified with ${}^\bullet r$. Thus $\mathbb{C}$ is viewed as a subfield of ${}^\bullet\mathbb{C}$. An element $u \in {}^\circ\mathcal{U}$ is *standard* if and only if $u = {}^\bullet x$ for some $x \in \mathcal{U}$. Thus ${}^\bullet\mathbb{N}$ and ${}^\bullet\mathbb{R}$ are standard sets *even though they have non-standard elements*. We denote the formula "x is standard" by $\mathrm{st}(x)$. We use the notation $\forall^{\mathrm{st}} x \Phi(x)$ and $\exists^{\mathrm{st}} x \Phi(x)$ which are abbreviations for the formulas $\forall x\ [\mathrm{st}(x) \implies \Phi(x)]$ and $\exists x\ [\mathrm{st}(x) \wedge \Phi(x)]$ respectively. More generally, if Φ is a first order formula, Φ^{st} is the formula where all quantifications of the form $\forall x$ and $\exists x$ are replaced with quantifications $\forall^{\mathrm{st}} x$ and $\exists^{\mathrm{st}} x$ respectively. The transfer principle then takes the form:

3.2. If $\Phi(x_1,\ldots,x_n)$ is a bounded formula whose free variables are among $x_1,\ldots,x_n$, then for all standard $a_1,\ldots,a_n \in {}^\circ\mathcal{U}$,

$$\Phi^{\mathrm{st}}(a_1,\ldots,a_n) \iff \Phi(a_1,\ldots,a_n).$$

Non-Standard analysis uses in an essential way non-standard integers. The following principle guarantees their existence:

3.3 (Countable Saturation). If $\{A_n : n \in \mathbb{N}\}$ is a sequence of internal sets in ${}^\circ\mathfrak{V}$ such that for all $n \in \mathbb{N}$ $A_1 \cap A_2 \cap \cdots \cap A_n$ is non-empty, then there is an internal element a such that $a \in A_n$ for all $n \in \mathbb{N}$.

Proposition 3.4. *${}^\bullet\mathbb{N} \setminus \mathbb{N}$ is non-empty.*

Proof. For finite subsets of $\mathfrak{V}$ we have ${}^\bullet\{a_1, \ldots, a_n\} = \{{}^\bullet a_1, \ldots, {}^\bullet a_n\}$. Now $\mathbb{N} \setminus \{1, \ldots, n\}$ is non-empty. Therefore for all $n \in \mathbb{N}$,

$$A_n = {}^\bullet\mathbb{N} \setminus \{1, \ldots, n\} \neq \emptyset$$

and thus there is an $a \in \bigcap_k A_k$. Such an a is distinct from all $k \in \mathbb{N}$. □

Countable saturation also implies:

Proposition 3.5. *$\mathbb{N}$ is an external subset of ${}^\bullet\mathbb{N}$.*

Proof. Suppose $\mathbb{N}$ is internal. Then $B_n = \mathbb{N} \setminus \{1, \ldots, n\}$ is non-empty and internal. Thus there is an $m \in \bigcap_k B_k$, that is $m \in \mathbb{N}$ such that $m > k$ for all $k \in \mathbb{N}$ which is absurd. □

Corollary 3.6. *Suppose A is an internal set such that $\mathbb{N} \subseteq A$. Then there exists $M \in ({}^\bullet\mathbb{N} \setminus \mathbb{N}) \cap A$.*

Stated another way:

Corollary 3.7. *If $\Phi(n)$ is a formula which holds for all standard integers n then it holds for at least one unbounded integer.*

Proposition 3.8. *For any sequence $\{a_n\}_{n\in\mathbb{N}}$ of elements of ${}^\circ\mathfrak{V}$ such that $a_n \in A$, there is an internal sequence $\{a'_n\}_{n\in{}^\bullet\mathbb{N}}$ which extends the original sequence, that is $a'_n = a_n$ for all $n \in \mathbb{N}$.*

Proof. For each $n \in \mathbb{N}$, let A_n be the set of sequences $\{b_k\}_{k\in{}^\bullet\mathbb{N}}$ which coincide with $\{a_k\}_{k\in\mathbb{N}}$ in the interval $\{1, 2, \ldots, n\}$. For all $n \in \mathbb{N}$, A_n is non-empty since we can exhibit an element $b \in A_n$ as follows:

$$b_k = \begin{cases} a_k & \text{if } k \leq n \\ 0 & \text{otherwise} \end{cases}$$

The sequence is internal, since it is defined by an internal formula. By countable saturation, there is an internal a that is an element of all the sets A_n. □

Definition 3.9. An $r \in {}^\bullet\mathbb{R}$ is *infinitesimal* if and only if for every $n \in \mathbb{N}$, $|r| \leq n^{-1}$.

Proposition 3.10. *There are infinitesimal real numbers.*

x is infinitesimal is written as $x \simeq 0$.

Proof. For $n \in \mathbb{N}$, let $A_n = \{r \in {}^\bullet\mathbb{R} : 0 \leq r \leq 1/n\}$. A_n is non-empty and this by countable saturation, $\bigcap_n A_n$ is non-empty. □

Definition 3.11. A positive hyperreal r is *infinite*, written as $x \simeq \infty$, if and only if $n \in \mathbb{N}$, $r \geq n$.

We use the notation $r \gg 0$ to indicate r is not infinitesimal and $r \ll \infty$ to indicate r is not infinite.

4. Non-standard view of computational derivability

A critical feature of a good model for tool-based protocol analysis is to focus on a single setting for computations. The computational model for exponentiation environments breaks this feature because of its use of the security parameter k. Our approach to resolving this tension is to use non-standard analysis to narrow our focus to a *single* k that can be used to express all the key properties. In particular, k will be greater than any finite number.

In this section, we show how to simplify the computational model in this way. First, we discuss the exponentiation environment we obtain when we consider an admissible system at an infinite k. Then, we tackle the more complicated problem of how to express the mechanisms around the exponentiation environment: families of non-uniform circuits, probabilities, and negligible functions.

4.1. **Infinite-index admissible systems.**

Remark 4.1 (Notation). Given any standard sequence $\mathcal{S} = \{S_k\}_{k\in\mathbb{N}}$, ${}^\bullet\mathcal{S}$ denotes the family indexed by ${}^\bullet\mathbb{N}$ obtained by applying the transfer operator to $\mathcal{S}$. The family ${}^\bullet\mathcal{S}$ can be viewed as extension of $\mathcal{S}$. By overloading of notation, we denote each term of the family ${}^\bullet\mathcal{S}$ by S_k.

Now let $\mathcal{S} = \{(G_j, g_j, p_j) : j \in \mathbb{N}\}$ be an admissible system of groups and generators; ${}^\bullet\mathcal{S}$ is a family indexed on ${}^\bullet\mathbb{N}$ which extends $\mathcal{S}$. By transfer, for each $k \in {}^\bullet\mathbb{N}$, G_k is a cyclic group, generated by g_k, of prime order p_k. In particular, exponentiation is defined as a mapping $G_k \times \mathbb{Z}/(p_k) \to G_k$. Now let $k \simeq \infty$. Then $p_k \simeq \infty$ due to growth requirements on the sequence $\{p_k\}_k$ in Definition 2.1. The internal characteristic of this field is $p_k \simeq \infty$.

4.2. **Non-standard mechanisms.**

In this section, we tackle the more complicated problem of how to express the mechanisms around the exponentiation environment. First, we discuss non-negligible functions.

4.2.1. *Non-standard view of negligibility.*

First, we prove the following proposition.

Proposition 4.2. *A necessary and sufficient condition a (standard) function f on $\mathbb{N}$ be negligible is that for all standard n and $k \simeq \infty$, $|{}^\bullet f(k)| \leq k^{-n}$.*

Proof. For necessity, suppose f is negligible and n is standard. By the definition of negligible

$$\exists^{\mathrm{st}}\ell\ \forall^{\mathrm{st}}k \geq \ell\ |{}^\bullet f(k)| \leq k^{-n}$$

is valid. Applying transfer, which is legitimate since it is applied to the innermost quantifier

$$\exists^{\mathrm{st}}\ell\ \forall k \geq \ell\ |{}^\bullet f(k)| \leq k^{-n}$$

In particular, if $k \simeq \infty$, $|{}^\bullet f(k)| \leq k^{-n}$ as claimed.

The proof of sufficiency relies on a common technique involving overspill and transfer. Suppose that for all $k \simeq \infty$ and all standard n, $|{}^\bullet f(k)| \leq k^{-n}$. In particular,

$$\forall \ell \simeq \infty\ \forall k \geq \ell\ |{}^\bullet f(k)| \geq k^{-n}$$

and thus by overspill,

$$\exists^{\mathrm{st}}\ell\ \forall k \geq \ell\ |{}^\bullet f(k)| \geq k^{-n}$$

By transfer

$$\exists^{\mathrm{st}}\ell\ \forall^{\mathrm{st}}k \geq \ell\ |{}^\bullet f(k)| \geq k^{-n}$$

which is the claim f is negligible. □

4.2.2. *Non-standard view of probability.* Let $\mathcal{X} = \{X_k\}_{k\in\mathbb{N}}$ be a sequence of finite sets. A sequence of subsets $A_k \subseteq X_k$ is *negligible* if and only if $\Pr_k(A_k)$ is negligible as a function of k, where $\Pr_k$ is the uniform probability measure on X_k.

We will consider any hyperfinite set X as a space equipped with the probability measure

$$\Pr(A) = \frac{{}^\bullet\operatorname{card} A}{{}^\bullet\operatorname{card} X} \tag{3}$$

Proposition 4.3. *Let $\{X_k\}_{k\in\mathbb{N}}$ be a sequence of finite sets. A necessary and sufficient condition a sequence $\{A_k\}_k$ of subsets be negligible is that for every standard m and $k \simeq \infty$*

$$\Pr(A_k) \leq k^{-m} \tag{4}$$

Proof. The proof of this follows the same lines as the proof of Proposition 4.2. □

Definition 4.4. Let $K \simeq \infty$. A hyperreal θ is K-negligible if and only if for all standard m, $|\theta| \leq K^{-m}$. A hyperreal θ is of order K if and only if there is a standard m, such that $|\theta| \leq K^{-m}$.

Remark 4.5. Any K-negligible number θ is infinitesimal, since $\theta \leq K^{-1}$ and K^{-1} is already infinitesimal. The converse is false, since K^{-1} is infinitesimal but not negligible. We introduce this stronger concept motivated by Proposition 4.3 and the transfer principle to translate the property of negligible sequence into a "limit" property of a single hyperfinite set.

Note that negligible is defined relative to a scale parameter K.

In the statement of Proposition 4.3 there is no relation assumed between the cardinality of X_k and k. If we assume X_k has an exponential growth, that is for some constants $0 < c \leq C < \infty$ and all k,

$$c \leq \frac{\operatorname{card} X_k}{2^k} \leq C$$

then we can rewrite (4) as for all $k \simeq \infty$, $\Pr_k(A_k)$ is $\log {}^\bullet\operatorname{card} A_k$ negligible.

4.2.3. *Non-standard view of computational derivability.* Last, we explore the idea of infinite indices in polynomially bounded non-uniform circuit families. This is done by applying the transfer operator to everything in sight. In keeping with our notation, we use ${}^\bullet\mathcal{C}$ to denote the class of circuits in the universe ${}^\circ\mathcal{U}$, ${}^\bullet|\cdot|$ denotes the size function.

If $\mathcal{A} = \{A_k\} \in \mathcal{PNC}$ is a standard polynomially bounded non-uniform circuit family, by transfer we simply think of A_k as being of size $\leq \rho(k)$ even when $k \simeq \infty$. Using non-standard analysis, we can restate the condition with a single infinite index.

In the following $\mathfrak{P}$ denotes the set of primes.

Proposition 4.6. *A derivation problem $(\bar\alpha, \beta)$ is* solvable *if and only if for some $k \simeq \infty$, there is a $p \in {}^\bullet\mathfrak{P}$ such that $0 \ll p/2^k \ll \infty$ and an $A \in {}^\bullet\mathcal{C}$ such that for some standard m, $|A| \leq k^m$ and*

$$\Pr[\bar x \leftarrow (\mathbb{Z}/(p)); v \leftarrow A(\bar\alpha(\bar x)) : v = \beta(\bar x)\}] \tag{5}$$

is not k-negligible.

Proof. If the derivation problem is solvable in the sense of Definition 2.6, then overspill implies the stated condition. Conversely, if the stated condition holds, there are $k \simeq \infty$, standard constants $0 < c \leq C < \infty$ such that $c \leq p/2^k \leq C$, a standard positive integer m and a circuit A such that $\rho(A) \leq k^m$

$$\Pr[\bar{x} \leftarrow (\mathbb{Z}/(p)); v \leftarrow A(\bar{\alpha}(\bar{x})) : v = \beta(\bar{x})\}] \geq k^{-m} \tag{6}$$

Therefore the following formula with standard parameters $\bar{\alpha}, \beta, c, C$ is valid in ${}^\circ\mathfrak{V}$:

$$\begin{aligned} &\forall^{\mathrm{st}}\ell,\ \exists k \geq \ell,\ \exists p \in {}^\bullet\mathfrak{P},\ \exists A \in {}^\bullet\mathcal{PNC}, \\ &\quad c \leq p/2^k \leq C \\ &\quad \text{and} \\ &\quad \Pr[\bar{x} \leftarrow (\mathbb{Z}/(p)); v \leftarrow A(\bar{\alpha}(\bar{x})) : v = \beta(\bar{x})\}] \geq k^{-m} \end{aligned} \tag{7}$$

By transfer, we obtain the following completely standard formula.

$$\begin{aligned} &\forall \ell \in \mathbb{N},\ \exists k \geq \ell,\ \exists p \in \mathfrak{P},\ \exists A \in \mathcal{PNC}, \\ &\quad c \leq p/2^k \leq C \\ &\quad \text{and} \\ &\quad \Pr[\bar{x} \leftarrow (\mathbb{Z}/(p)); v \leftarrow A(\bar{\alpha}(\bar{x})) : v = \beta(\bar{x})\}] \geq k^{-m} \end{aligned} \tag{8}$$

This is precisely the condition for solvability. □

Note that since Proposition 4.6 refers only to a single infinite k, and since the properties observed in subsection 4.1 apply to any infinite k, this allows us to view the environment in the simple way we described at the beginning of this section: as a single environment, with no overly specific properties.

5. Formalized environments

The main aim of this paper is to obtain a formalized environment in which we can express Diffie-Hellman operations. We have thus far discussed only computational environments of this kind. For the purposes of automated analysis, we must make a Dolev-Yao style assumption on our environment, which would replace arbitrary adversary behavior with a more restricted set of such behavior based on expected derivations. Clearly, we will want to set our computation in G_k for an infinite k; for simplicity we refer to such a group as G.

Now, we will certainly want to represent the field of exponents $\mathbf{E} = \mathbb{Z}/(p)$. We would represent each independently chosen random value in $\mathbf{E}$ as a variable, and consider an adversary capable of exponentiation, field operations within $\mathbf{E}$, and group operations in G, based on knowing g as well as whatever input information is available.

Certainly, formal derivability of $\bar{\beta}$ from $\bar{\alpha}$ would be a well-defined alternative to the notion of derivation problem solvability. We seek a stronger justification of our choice of formalization, namely, that formalizing *transforms* solvability into formal derivability. The rest of the section deals with this aspect of formalization.

In Figure 1, we give a schematic of the models under discussion. If we were to approach D only through B, we gain little evidence that our choice of formalization is justified, but since B is fairly simple, we *do* get a good model to justify. We then aim to justify this choice of formalization by attempting the same kind of formalization on the regular computational model A, obtaining C, and only *then*

generalizing to infinite index. The main result of this section is that this alternate approach leads to the same notion of derivability.

5.1. **Formalizing the computational model.** Here, we must make a decision about how to properly translate the notion of derivation by a family of circuits to a formal one. We describe the formal derivation environment for each exponentiation environment in an admissible system of groups and generators $\mathcal{S} = \{(G_j, g_j, p_j) : j \in \mathbb{N}\}$ as defined in §4.1. Essentially, a derivation is a rational expression on exponents or exponents and bases. Rather than a polynomial bound on the circuit family, we require that the rational expressions involved are of *log-sublinear* degree: in other words, the expressions are of degree significantly less than p. A function $f : \mathbb{R} \longrightarrow \mathbb{R}$ is *log-sublinear* if and only if for every $k \in \mathbb{N}$,

$$\lim_{r\to\infty} \frac{f(r)}{r(\log r)^{-k}} = 0. \tag{9}$$

For example, any function such that $f(r) = O(r^{1-\varepsilon})$ for positive ε is log-sublinear. This is a very conservative restriction, because the expressions can still grow exponentially in k.

5.2. **Base and Exponent Schema.** For the Diffie-Hellman protocol, expressions are of two kinds: a set $\mathcal{U}$ of "bases" and $\mathcal{E}$ of "exponents". The derivation process is given as closure rules for the sets $U \subseteq \mathcal{U}$ and $E \subseteq \mathcal{E}$ known to the adversary:

(1) If $u, v \in U$ then $u \cdot v \in U$.
(2) If $R(\bar{x}) \in \mathbb{Z}(x_1, \ldots, x_n)$ is a rational expression with integer coefficients and $\bar{t} = t_1, \ldots, t_n \in E$ then $R(\bar{t}) \in E$.
(3) If $u \in U$ and $t \in E$, then $u^t \in U$.

Base and exponent expressions are intended to model uniform schemas specific to Diffie-Hellman. Formally, a *base and exponent schema* is a pair $(\mathbf{U}, \mathbf{E})$ where $\mathbf{U}$ is a set of base variables $\mathbf{E}$ is a set of exponent variables. In the following $\bar{u} = \langle u_1, \ldots, u_m \rangle$ is a sequence of base variables and $\bar{x} = \langle x_1, \ldots, x_n \rangle$ is sequence of exponent variables.

(1) The set of *exponent expressions* $\mathcal{E}$ consists of rational expressions $R(\bar{x}) \in \mathbb{Z}(\bar{x})$ in exponent variables.
(2) The set of *base expressions* consists of monomials
$$F(\bar{u}, \bar{x}) = u_1^{R_1(\bar{x})} u_2^{R_2(\bar{x})} \cdots u_n^{R_n(\bar{x})}$$
where $\bar{u}$ are base variables and $\bar{x}$ are exponent variables. We denote the set of base expressions in the variables $\bar{u}, \bar{x}$ by $\mathrm{B}\langle \bar{u}, \bar{x} \rangle$.

The equality relation between base expressions is purely formal:

$$u_1^{R_1(\bar{x})} u_2^{R_2(\bar{x})} \cdots u_n^{R_n(\bar{x})} = u_1^{S_1(\bar{x})} u_2^{S_2(\bar{x})} \cdots u_n^{S_n(\bar{x})}$$

if and only if $R_i(\bar{x}) = S_i(\bar{x})$. Later we will provide a semantics for equality which justifies this definition.

A *pure Diffie-Hellman term* is either an exponent expression or a base expression. Derivability is characterized by a set of closure rules for the set U of base expressions and E of exponent expressions known to the adversary. The closure rules are as follows:

(1) Suppose $R_1(\bar{x}), \ldots R_m(\bar{x}) \in E$. Then for any rational expression $S(\bar{y})$
$$S(R_1(\bar{x}), \ldots R_m(\bar{x})) \in E.$$

(2) If $u_1^{Q_1(\bar{x})}, u_2^{Q_1(\bar{x})}, \ldots, u_m^{Q_m(\bar{x})} \in B$ and $R_1(\bar{x}), \ldots R_m(\bar{x}) \in E$ then

$$u_1^{Q_1(\bar{x})R_1(\bar{x})} \cdots u_m^{Q_m(x)R_m(\bar{x})} \in B$$

5.3. **Derivability definitions and propositions.** Recall that our formalized version of a non-uniform family of circuits is a non-uniform family of rational expressions.

Definition 5.1. Suppose $R \in \mathbb{Z}(x_1, \ldots, x_n)$ and $\{S_k\}_{k\in\mathbb{N}}$ is a sequence of elements of $\mathbb{Z}(x_1, \ldots, x_n)$. $R \sim \{S_k\}_k$ if and only if there is a non-negligible function ε such that for all $k \in \mathbb{N}$,

$$\Pr_k \underbrace{\{\bar{\sigma} \in (\mathbb{Z}/(p_k))^n : R(\bar{\sigma}) = S_k(\bar{\sigma})\}}_{A_k} \geq \varepsilon(k) \tag{10}$$

Remark 5.2. In (10), the symbol $\Pr_k$ refers to the uniform probability measure on $(\mathbb{Z}/(p_k))^n$. Implicit in the defining condition for the sets A_k is that both the RHS and the LHS of the equation within the braces are defined. In particular, the denominators of both $R(\bar{\sigma})$ and $S_k(\bar{\sigma})$ must be non-zero in order for $\bar{\sigma}$ to be an element of A_k.

Remark 5.3. A necessary and sufficient condition that $R \sim \{S_k\}_k$ is that there exist an $m \in \mathbb{N}$ such that

$$\Pr_k \underbrace{\{\bar{\sigma} \in (\mathbb{Z}/(p_k))^n : R(\bar{\sigma}) = S_k(\bar{\sigma})\}}_{A_k} \geq (\log p_k)^{-m} \tag{11}$$

for infinitely many k. This is a trivial rewrite of (10) using Remark 2.2.

Proposition 5.4. *Suppose $R_\beta, R_\alpha, S_k \in \mathbb{Z}(x_1, \ldots, x_n)$ and $R_\beta \sim \{S_k \circ R_\alpha\}_k$. If the degree of S_k is a log-sublinear function of p_k (that is the degrees of the numerator and denominator of S_k are log-sublinear in p_k) as $k \to \infty$ then there is an $S \in \mathbb{Z}(x_1, \ldots, x_n)$ such that $S \circ R_\alpha = R_\beta$.*

In other words, when such an $\{S_k\}$ family exists for a given (α, β) exponent-only derivability problem, R_β can be derived from R_α.

Next we state the more general notion which includes both base and exponent expressions and state the equivalent proposition.

Definition 5.5. Suppose $\bar{u} \in \mathbf{U}^m, \bar{x} \in \mathbf{E}^n$, $F(\bar{u}, \bar{x}) \in \mathrm{B}\langle\bar{u}, \bar{x}\rangle$ and $\{G_k(\bar{u}, \bar{x})\}_{k\in\mathbb{N}}$ a sequence of elements of $\mathrm{B}\langle\bar{u}, \bar{x}\rangle$. Then $F \sim \{G_k\}_k$ if and only if there is a non-negligible function ε such that for all $k \in \mathbb{N}$,

$$\Pr_k\{(\bar{\tau}, \bar{\sigma}) \in (\mathbb{Z}/(p_k))^m \times (\mathbb{Z}/(p_k))^n : F(\bar{\tau}, \bar{\sigma}) = G_k(\bar{\tau}, \bar{\sigma})\} \geq \varepsilon(k). \tag{12}$$

Proposition 5.6. *Suppose $R_\beta, R_\alpha, S_k \in \mathrm{B}\langle\bar{u}, \bar{x}\rangle$ and $R_\beta \sim \{S_k \circ R_\alpha\}_k$. If the degree of S_k is log-sublinear in k then there exists $S \in \mathrm{B}\langle\bar{u}, \bar{x}\rangle$ such that $R_\beta = S \circ R_\alpha$.*

Propositions 5.4 and 5.6 are proved in the next section.

5.4. **Generalizing to infinite index.** The formalized version of the computational model of derivability is stated in Definitions 5.1 and 5.5. These definitions and the key results Propositions 5.4 and 5.6 are formulated in completely standard terms. We apply non-standard analysis techniques, in particular the transfer principle to extend these definitions and propositions to infinite k. By applying the overspill principle we can then isolate these statements to a single, infinite k.

This produces *almost* the environment we expect; the one difference is that we get a definition of solvable based on a non-negligible probability of success of being solved by an allowable derivation, rather than being exactly solved by it. However, we are able to prove that these amount to the same thing. In order to do this, we require some preliminary concepts that restrict the size of algebraic varieties over finite fields.

5.5. **Varieties and Negligible Sets.** Let $\mathbf{F}$ be an internal field. We consider *internal* multivariate polynomials $P \in \mathbf{F}[x_1, \ldots, x_n]$ where $n \in {}^\bullet\mathbb{N}$. Elements of $\mathbf{F}[x_1, \ldots, x_n]$ are *internal functions* from the free internal Abelian semigroup generated by $x_1, \ldots, x_n$ into the field $\mathbf{F}$. We also use the notation $\mathbf{F}[\bar{x}]$ to denote the ring $\mathbf{F}[x_1, \ldots, x_n]$. An element $P \in \mathbf{F}[x_1, \ldots, x_n]$ defines a function $\mathbf{F}^n \longrightarrow \mathbf{F}$ which by abuse of language we also denote by P. Note that in general distinct polynomials can define the same function.

Now suppose $\mathbf{F}$ is a *hyperfinite* field and $P \in \mathbf{F}[x_1, \ldots, x_n]$ is a polynomial of degree m. The *variety* defined by P is the set $E \subseteq \mathbf{F}^n$

$$E = \{(x_1, \ldots, x_n) \in \mathbf{F}^n : P(x_1, \ldots, x_n) = 0\} \tag{13}$$

If f is log-sublinear, then for $R \simeq \infty$ and standard hyperinteger k,

$$\frac{{}^\bullet f(R)}{R(\log R)^{-k}} \simeq 0. \tag{14}$$

An internal set $E \subseteq X$ is *negligible* if and only if $\Pr(E)$ is negligible relative to the scale parameter $\log {}^\bullet\mathrm{card}\, X$. The key result we use is the following:

Proposition 5.7. *Suppose $E \subseteq \mathbf{F}^n$ is an algebraic variety defined by a non-trivial polynomial P such that*

$$\deg P \leq {}^\bullet f({}^\bullet\mathrm{card}\, \mathbf{F}) \tag{15}$$

where f is log-sublinear. Then E is negligible.

The result is proved in §7.

Remark 5.8. Note that the degree of P need not be standard. Stated contrapositively, Proposition 5.7 states that if P defines a variety which is non-negligible, then P is trivial.

Remark 5.9. Stated contrapositively, Proposition 5.7 states that two polynomials whose degrees are not too large (in the sense of the inequality (15)) and which agree on a non-negligible set are in fact identical.

6. Derivability in the Formal Model

Fix a derivability problem and let U, E be the sets of base and exponent expressions derivable by the adversary. In other words, U and E consist of base and exponent expressions obtained by composing rational expressions with the R_α values. We use the notation and context of §4.1, in particular $\mathcal{S} = \{(G_j, g_j, p_j) : j \in \mathbb{N}\}$ is an admissible system of groups and generators and ${}^\bullet\mathcal{S}$ is the extension obtained by transfer. The following remark is crucial in what follows:

Remark 6.1. Suppose F is standard and $F \in {}^\bullet U$ (respectively $F \in {}^\bullet E$). Then $F \in U$ (respectively $F \in E$). This is immediate from the transfer principle.

The previous remark is the basic idea behind our use of non-standard analysis. We first consider exponent expressions:

Proof of Proposition 5.4. Since the set of $\{p_j : j \in \mathbb{N}\}$ is unbounded, there is an $M \simeq \infty$ such that $p_M \simeq \infty$ and

$$R(\bar{\sigma}) - S_M(\bar{\sigma}) = 0 \tag{16}$$

for $\bar{\sigma} \in ({}^\bullet\mathbb{Z}/(p_M))^n$ on a non-negligible set A_M. Let

$$R(\bar{x}) = \frac{R^{\text{num}}(\bar{x})}{R^{\text{den}}(\bar{x})}, \quad S_M(\bar{x}) = \frac{S^{\text{num}}(\bar{x})}{S^{\text{den}}(\bar{x})} \tag{17}$$

so (16) can be regarded as the conjunction

(1) $R^{\text{den}}(\bar{\sigma})$ and $S^{\text{den}}(\bar{\sigma})$ are non-zero
(2) $R^{\text{num}}(\bar{\sigma})S^{\text{den}}(\bar{\sigma}) = S^{\text{num}}(\bar{\sigma})R^{\text{den}}(\bar{\sigma})$

The result now follows from Proposition 5.7 and the transfer principle. □

Proof of Proposition 5.6. There is an $M \simeq \infty$ such that $p_M \simeq \infty$ and the set

$$\{(\bar{\tau}, \bar{\sigma}) \in ({}^\bullet\mathbb{Z}/(p_M))^m \times ({}^\bullet\mathbb{Z}/(p_M))^n : F(\bar{\tau}, \bar{\sigma}) = G_M(\bar{\tau}, \bar{\sigma})\}$$

has non-negligible probability. Equivalently $(\bar{\tau}, \bar{\sigma}) \in ({}^\bullet\mathbb{Z}/(p_M))^m \times ({}^\bullet\mathbb{Z}/(p_M))^n$ such that

$$\tau_1^{R_1(\bar{\sigma})} \cdots \tau_m^{R_m(\bar{\sigma})} = \tau_1^{S_1(\bar{\sigma})} \cdots \tau_m^{S_m(\bar{\sigma})} \tag{18}$$

has non-negligible probability, where

$$G_M(\bar{u}, \bar{x}) = u_1^{S_1(\bar{x})} \cdots u_m^{S_m(\bar{x})}$$

Choose a generator ρ for G_M. Then (18) can be expressed as

$$\rho^{\alpha_1 R_1(\bar{\sigma}) + \cdots + \alpha_m R_m(\bar{\sigma})} = \rho^{\alpha_1 S_1(\bar{\sigma}) + \cdots + \alpha_m S_m(\bar{\sigma})} \tag{19}$$

which holds for $(\bar{\alpha}, \bar{\sigma})$ ranging over a subset A_M of $({}^\bullet\mathbb{Z}/(p_M))^m \times ({}^\bullet\mathbb{Z}/(p_M))^n$ of non-negligible probability. Therefore

$$\alpha_1(R_1(\bar{\sigma}) - S_1(\bar{\sigma})) + \cdots + \alpha_m(R_m(\bar{\sigma}) - S_m(\bar{\sigma})) = 0.$$

for $(\bar{\alpha}, \bar{\sigma}) \in A_M$. Thus for all k, $1 \leq k \leq m$, $R_k(\bar{x}) - S_k(\bar{x}) = 0$ which proves the result. □

7. Negligibility of Algebraic Varieties

We now turn to the main technical result which limits the size of algebraic varieties defined by polynomials of log-sublinear degree in the field size.

Proposition 7.1. *Suppose $E \subseteq \mathbf{F}^n$ is an algebraic variety defined by a non-trivial polynomial P. Then*

$${}^\bullet\text{card}\, E \leq n \deg P ({}^\bullet\text{card}\, \mathbf{F})^{n-1} \tag{20}$$

Proof. Let $m = \deg P$. The proof is by induction on n. P is of the form

$$P(\bar{x}, y) = {}^\bullet\sum\nolimits_{k \leq m} a_k P_k(\bar{x}) y^k, \tag{21}$$

where $P_k(\bar{x}) \in \mathbf{F}[x_1, \ldots, x_{n-1}]$ is a polynomial of degree at most m. Now for each $\bar{a} \in \mathbf{F}^{n-1}$, one of the following holds:

(1) The polynomial in one variable $P(\bar{a}, y)$ is identically 0 or equivalently,

$$P_0(\bar{a}) = P_1(\bar{a}) = \cdots = P_m(\bar{a}) = 0.$$

By the inductive hypothesis there are at most $(n-1) \times m \times ({}^\bullet\mathrm{card}\,\mathbf{F})^{n-2}$ elements $\bar{a} \in \mathbf{F}^{n-1}$ in this case and each one contributes ${}^\bullet\mathrm{card}\,\mathbf{F}$ solutions to $P(\bar{a}, b) = 0$

(2) There are possibly as many as $({}^\bullet\mathrm{card}\,\mathbf{F})^{n-1}$ elements $\bar{a}$ in this case, but each one contributes at most m solutions to $P(\bar{a}, b) = 0$ as b ranges over $\mathbf{F}$.

Altogether therefore, there are at most

$$(n-1)m({}^\bullet\mathrm{card}\,\mathbf{F})^{n-1} + ({}^\bullet\mathrm{card}\,\mathbf{F})^{n-1}m = nm({}^\bullet\mathrm{card}\,\mathbf{F})^{n-1}$$

elements in E. In case (1), therefore $P(\bar{a}, b) = 0$ has at most $({}^\bullet\mathrm{card}\,\mathbf{F})^{n-1} \times m$ solutions as $\bar{a}, b$ range over $\mathbf{F}^{n-1}$, $\mathbf{F}$ respectively. □

Henceforth we assume without further mention that $\mathbf{F}$ is a hyperfinite field such that ${}^\bullet\mathrm{card}\,\mathbf{F} \simeq \infty$. In this section, $\mathbf{F}$ will be instantiated with a field ${}^\bullet\mathbb{Z}/(p)$ with p a infinite prime.

Proof of Proposition 5.7. Let $m = \deg P$. By Proposition 7.1 and the assumption that ${}^\bullet\mathrm{card}\,\mathbf{F} \simeq \infty$,

$$\begin{aligned}
\Pr(E)(\log {}^\bullet\mathrm{card}\,\mathbf{F})^k &= \frac{{}^\bullet\mathrm{card}\,E}{{}^\bullet\mathrm{card}\,\mathbf{F}^n}(\log {}^\bullet\mathrm{card}\,\mathbf{F})^k \\
&\leq \frac{nm\,{}^\bullet\mathrm{card}\,\mathbf{F}^{n-1}}{{}^\bullet\mathrm{card}\,\mathbf{F}^n}(\log {}^\bullet\mathrm{card}\,\mathbf{F})^k \\
&\leq n\,\frac{f({}^\bullet\mathrm{card}\,\mathbf{F})}{{}^\bullet\mathrm{card}\,\mathbf{F}}(\log {}^\bullet\mathrm{card}\,\mathbf{F})^k \simeq 0.
\end{aligned}$$

□

A partial internal function f is *defined almost everywhere* if and only if $X \setminus \mathrm{dom}\, X$ is negligible.

Proposition 7.2. *Suppose* $\mathbf{F}$ *is a hyperfinite field such that* ${}^\bullet\mathrm{card}\,\mathbf{F} \in {}^\bullet\mathbb{N} \setminus \mathbb{N}$ *and* $R(\bar{x}) = P(\bar{x})/Q(\bar{x})$ *where* $0 \neq Q(\bar{x}) \in \mathbf{F}[x]$ *and* $\deg Q(\bar{x}) \leq Cf({}^\bullet\mathrm{card}\,\mathbf{F})$ *with* nf *log-sublinear. Then* R *is almost everywhere defined.*

Proof. P is defined precisely when $Q(\bar{x}) \neq 0$ which by Proposition 5.7 holds almost everywhere. □

8. Restricting to the Diffie-Hellman algebra

The full Diffie-Hellman model thus far developed unfortunately falls short of what we need for protocol analysis. As Dougherty and Guttman point out, the notion that all exponents other than 0 have inverses cannot be simply expressed in an equational theory [4]. Worse, any reasonable attempt at emulating this formal model with an algebra would be problematic because the exponents would form a ring structure, and unification, a key technique in automated exploratory protocol analysis, is not known to be decidable for rings. Thus, we restrict our formal model to a weaker one which does not capture exponent addition or group multiplication.

Sorts

Sorts:	BASE, EXPN	

Operations

$(\cdot)^{(\cdot)}$	BASE × EXPN → BASE	Exponentiation
$\cdot\,\cdot$	EXPN × EXPN → AKEY	Multiplication
$(\cdot)^{-1}$	EXPN → EXPN	Inverse

Constants

1	EXPN	Identity

Equations

$g^{xy} \equiv (g^x)^y$	g: BASE, x, y: EXPN
$xy \equiv yx$	x, y: EXPN
$x(yz) \equiv (xy)z$	x, y, z: EXPN
$g^1 \equiv g$	g: BASE
$1x \equiv x$	x: EXPN
$x(x^{-1}) \equiv 1$	x: EXPN

FIGURE 2. Our restricted Diffie-Hellman algebra

8.1. **Our Diffie-Hellman Algebra.** Our Diffie-Hellman algebra is illustrated in Figure 2. This algebra emulates a restricted version of our Diffie-Hellman model in which addition of exponents and multiplication of bases are not included. Unification in our algebra is efficiently computable and is unitary [5].

In this section, we present the similarly restricted version of our Diffie-Hellman model, and justify our restriction in the following sense. In the restricted model, we can formulate fewer formal solvability statements than in the full model. However, all formal solvability statements in the restricted model are true exactly if they are true in the full model.

The results of Proposition 8.2 and Corollary 8.3 are the main results supporting this conclusion.

8.2. **Monomials and Polynomials.** Suppose $r, n \in \mathbb{Z}$ and $A \in \mathbf{M}_{r\times n}(\mathbb{Z})$. Let

$$A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{r1} & \alpha_{r2} & \cdots & \alpha_{rn}. \end{bmatrix} = \begin{bmatrix} A_1 \\ A_2 \\ \vdots \\ A_r \end{bmatrix} \tag{22}$$

$\overline{M}_A(\bar{x})$ is the vector of monomials (displayed as a column vector for readability):

$$\overline{M}_A(\bar{x}) = \begin{bmatrix} M_{A_1}(\bar{x}) \\ M_{A_2}(\bar{x}) \\ \vdots \\ M_{A_r}(\bar{x}) \end{bmatrix} = \begin{bmatrix} x_1^{\alpha_{11}} x_2^{\alpha_{12}} \cdots x_n^{\alpha_{1n}} \\ x_1^{\alpha_{21}} x_2^{\alpha_{22}} \cdots x_n^{\alpha_{2n}} \\ \vdots \\ x_1^{\alpha_{r1}} x_2^{\alpha_{r2}} \cdots x_n^{\alpha_{rn}} \end{bmatrix} \tag{23}$$

As a special case, if $\bar{\alpha} \in \mathbf{M}_{1\times n}(\mathbb{Z})$ (i.e. $\bar{\alpha}$ is a row vector with n entries), then

$$M_{\bar{\alpha}}(\bar{x}) = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$$

We regard $\overline{M}_A(\bar{x})$ as a mapping $\mathbf{F}^n \longrightarrow \mathbf{F}^r$. Since each component M_ℓ of $\overline{M}_A$ is almost everywhere defined and the number of components is standard, $\overline{M}_A$ is almost everywhere defined. The proof of the following is a straightforward computation:

Proposition 8.1. *If $C \in \mathbf{M}_{r\times n}(\mathbb{Z})$ and $D \in \mathbf{M}_{r\times n}(\mathbb{Z})$ then*

$$\overline{M}_C(\bar{x}) \cdot \overline{M}_D(\bar{x}) = \overline{M}_{C+D}(\bar{x}) \tag{24}$$

where the product is the coordinatewise product. If $B \in \mathbf{M}_{s\times r}(\mathbb{Z})$ and $A \in \mathbf{M}_{r\times n}(\mathbb{Z})$, then

$$\overline{M}_B\left(\overline{M}_A(\bar{x})\right) = \overline{M}_{B\cdot A}(\bar{x}). \tag{25}$$

In particular, if $\bar{\beta} \in \mathbf{M}_{1\times r}(\mathbb{Z})$

$$\overline{M}_{\bar{\beta}\cdot A}(\bar{x}) = M_{\bar{\beta}}\overline{M}_A(\bar{x}) = M_{A_1}^{\beta_1}(\bar{x})M_{A_2}^{\beta_2}(\bar{x})\cdots M_{A_r}^{\beta_r}(\bar{x}) \tag{26}$$

We now consider composition with polynomials. Suppose $P(\bar{y}) \in \mathbf{F}[y_1, \ldots, y_r]$ is a polynomial of degree m. Thus

$$P(y_1, \ldots, y_r) = \sum_{|\bar{\beta}|\le m} c_{\bar{\beta}} y_1^{\beta_1} y_2^{\beta_2} \cdots y_r^{\beta_r} = \sum_{|\bar{\beta}|\le m} c_{\bar{\beta}} M_{\bar{\beta}}(\bar{y}) \tag{27}$$

If A is an $r \times n$ matrix as in (22), then by (26),

$$\begin{aligned} P\left(\overline{M}_A(\bar{x})\right) &= \sum_{|\bar{\beta}|\le m} c_{\bar{\beta}} M_{\bar{\beta}}(M_A(\bar{x})) \\ &= \sum_{\bar{\beta}} c_{\bar{\beta}} M_{\bar{\beta}\cdot A}(\bar{x}) \\ &= \sum_{\bar{\gamma}} \left\{ \sum_{\bar{\beta}\cdot A=\bar{\gamma}} c_{\bar{\beta}} \right\} M_{\bar{\gamma}}(\bar{x}). \end{aligned}$$

Since the family $M_{\bar{\gamma}}(\bar{x})$ of monomials in the vector space $\mathbf{F}[x_1, \ldots, x_n]$ is linearly independent, we have shown:

Proposition 8.2. *If $P(\bar{y}) = \sum_{\bar{\beta}} c_{\bar{\beta}} \bar{y}^{\bar{\beta}} \in \mathbf{F}[y_1, \ldots, y_r]$ and $A \in \mathbf{M}_{r\times n}(\mathbb{Z})$ is such that*

$$P\left(M_{A_1}(\bar{x}), M_{A_2}(\bar{x}), \ldots, M_{A_r}(\bar{x})\right) = 0$$

then for every $\bar{\gamma}$,

$$\sum_{\bar{\beta}\cdot A=\bar{\gamma}} c_{\bar{\beta}} = 0. \tag{28}$$

An immediate corollary is the conclusion that polynomial identities between monomials are essentially monomial identities. This result has the following significance: an adversary that can compute arbitrary polynomials on monomials has no advantage over an adversary that is restricted to computing monomials.

Corollary 8.3. *Suppose*

$$R(\bar{y}) = \frac{\sum_{\bar{\beta}} c_{\bar{\beta}} M_{\bar{\beta}}(\bar{y})}{\sum_{\bar{\beta}} d_{\bar{\beta}} M_{\bar{\beta}}(\bar{y})} \in \mathbf{F}(y_1, \ldots, y_r), \tag{29}$$

$A \in \mathbf{M}_{r\times n}(\mathbb{Z})$ and $\bar{\gamma} \in \mathbf{M}_{1\times n}(\mathbb{Z})$ are such that

$$R\left(M_{A_1}(\bar{x}), M_{A_2}(\bar{x}), \ldots, M_{A_r}(\bar{x})\right) = M_{\bar{\gamma}}(\bar{x}) \tag{30}$$

Then there is a $\bar{\tau} \in \mathbf{M}_{1\times r}(\mathbb{Z})$ *such that* $\bar{\gamma} = \bar{\tau} \cdot A$ *and for any such* $\bar{\tau}$

$$M_{A_1}^{\tau_1}(\bar{x}) M_{A_2}^{\tau_2}(\bar{x}) \cdots M_{A_r}^{\tau_r}(\bar{x}) = M_{\bar{\tau}}(\overline{M}_A(\bar{x})) = M_{\bar{\gamma}}(\bar{x}). \tag{31}$$

Proof. From (29) and (30) it follows that

$$\begin{aligned}\sum_{\bar{\beta}} d_{\bar{\beta}} M_{\bar{\gamma}+\bar{\beta}\cdot A}(\bar{x}) &= M_{\bar{\gamma}}(\bar{x}) \sum_{\bar{\beta}} d_{\bar{\beta}} M_{\bar{\beta}}(\overline{M}_A(\bar{x})) \\ &= \sum_{\bar{\beta}} c_{\bar{\beta}} M_{\bar{\beta}}(\overline{M}_A(\bar{x})) \\ &= \sum_{\bar{\beta}} c_{\bar{\beta}} M_{\bar{\beta}\cdot A}(\bar{x})\end{aligned}$$

By Proposition 8.2, for every $\bar{\tau}$,

$$\sum_{\bar{\gamma}+\bar{\beta}\cdot A=\bar{\tau}} d_{\bar{\beta}} M_{\bar{\gamma}+\bar{\beta}\cdot A}(\bar{x}) = \sum_{\bar{\beta}\cdot A=\bar{\tau}} c_{\bar{\beta}} M_{\bar{\beta}\cdot A}(\bar{x}) \tag{32}$$

Let $\bar{\tau}$ be such that $\sum_{\bar{\gamma}+\bar{\beta}\cdot A=\bar{\tau}} d_{\bar{\beta}} \neq 0$. Such a $\bar{\tau}$ exists, for otherwise the rational function R would be identically 0 which is impossible by (30). Choose some $\bar{\rho}$ such that $\bar{\gamma} + \bar{\rho} \cdot A = \bar{\tau}$; such an index exists for otherwise the sum $\sum_{\bar{\gamma}+\bar{\beta}\cdot A=\bar{\tau}} d_{\bar{\beta}}$ would be 0. If $\bar{\gamma} + \bar{\beta} \cdot A = \bar{\tau}$, then

$$M_{\bar{\gamma}+\bar{\rho}\cdot A}(\bar{x}) = M_{\bar{\gamma}+\bar{\beta}\cdot A}(\bar{x}).$$

Similarly choose some $\bar{\kappa}$ such that $\bar{\kappa} \cdot A = \tau$. If $\bar{\beta} \cdot A = \bar{\tau}$

$$M_{\bar{\kappa}\cdot A}(\bar{x}) = M_{\bar{\tau}}(\bar{x}) = M_{\bar{\beta}\cdot A}(\bar{x})$$

Then from (32).

$$\Big(\sum_{\bar{\gamma}+\bar{\beta}\cdot A=\bar{\tau}} d_{\bar{\beta}}\Big) M_{\bar{\gamma}+\bar{\rho}\cdot A}(\bar{x}) = \Big(\sum_{\bar{\beta}\cdot A=\bar{\tau}} c_{\bar{\beta}}\Big) M_{\bar{\kappa}\cdot A}(\bar{x}) \tag{33}$$

Thus

$$\begin{aligned}M_{\bar{\gamma}}(\bar{x}) &= \frac{\sum_{\bar{\beta}\cdot A=\bar{\tau}} c_{\bar{\beta}}}{\sum_{\bar{\gamma}+\bar{\beta}\cdot A=\bar{\tau}} d_{\bar{\beta}}} \frac{M_{\bar{\kappa}\cdot A}(\bar{x})}{M_{\bar{\rho}\cdot A}(\bar{x})} \\ &= \frac{\sum_{\bar{\beta}\cdot A=\bar{\tau}} c_{\bar{\beta}}}{\sum_{\bar{\gamma}+\bar{\beta}\cdot A=\bar{\tau}} d_{\bar{\beta}}} M_{A_1}^{\kappa_1-\rho_1}(\bar{x}) M_{A_2}^{\kappa_2-\rho_2}(\bar{x}) \cdots M_{A_r}^{\kappa_r-\rho_r}(\bar{x})\end{aligned}$$

which is of the form (31). □

9. Conclusion

In this paper we justify a simple algebra for the modeling of Diffie-Hellman protocols. The algebra represents multiplication of exponents and exponentiation but does not represent addition of exponents or multiplication of bases. We justify our model by linking it to a standard computational model, and show a link between the concept of derivability in the computational model and in our model. The link involves two transformations of the model: a Dolev-Yao-style formalization and a generalization to hyperfinite parameters. We show that either order of these two steps leads to the same notion of derivability.

We then consider the restriction to monomial derivations (that is, derivations that act as monomials on exponents) and show a conservative extension result,

namely, that the fuller model including multiplication of bases and addition of exponents is a conservative extension of our restricted model. This allows us to conclude that for problems that may be expressed in our restricted model, derivability in the restricted model is equivalent to derivability in the unrestricted model.

References

[1] S. Albeverio, J.E. Fenstad, R. Höegh-Kron, and T. Lindström. *Nonstandard Analysis in Stochastic Analysis and Mathematical Physics*. Academic Press, New York, 1986.

[2] Ran Canetti. *Encyclopedia of Cryptography and Security*, chapter Decisional Diffie-Hellman Assumption. Springer-Verlag, 2005.

[3] W. Diffie and M. Hellman. New directions in cryptography. *Information Theory, IEEE Transactions on*, 22(6):644 – 654, nov 1976.

[4] Daniel J. Dougherty and Joshua D. Guttman. Symbolic protocol analysis for Diffie-Hellman. *CoRR*, abs/1202.2168, 2012.

[5] Catherine Meadows and Paliath Narendran. A unification algorithm for the group diffie-hellman protocol. In *IN PROC. OF WITS 2002*, pages 14–15, 2002.

[6] Edward Nelson. Internal set theory: A new approach to nonstandard analysis. *Bull. Amer. Math. Soc*, pages 1165–1198, 1977.

Asymptotic Results via Non-standard Analysis

Proposition .1. *A necessary and sufficient condition a function f be non-negligible is that there exist a a standard n and $K \simeq \infty$ such that $|^\bullet f(K)| \geq K^{-n}$.*

Proof. For $n \in \mathbb{N}$, then set In one direction apply overspill. In the other direction

$$\forall^{\mathrm{st}} k \; \exists K \geq k \; |^\bullet f(K)| \geq K^{-n}$$

is valid. By transfer

$$\forall^{\mathrm{st}} k \; \exists^{\mathrm{st}} K \geq k \; |^\bullet f(K)| \geq K^{-n}$$

is valid. However, if K is standard $^\bullet f(K) = f(K)$. □